The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/10/2016

SUBJECT:
Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution (MS16-055)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Windows, the most severe of which could allow for remote code execution. These vulnerabilities can be exploited by either convincing a user to open a specially crafted document or convincing a user to visit a specially crafted webpage. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Windows Vista
- Windows Server 2008, 2008 R2 (Including Server Core installations)
- Windows 7
- Windows 8.1, RT 8.1
- Windows Server 2012, 2012 R2 (Including Server Core installations)
- Windows 10

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities exist in Microsoft Windows, the most severe of which could allow remote code execution. The vulnerabilities are as follows:

- Multiple information disclosure vulnerabilities exist when the Windows GDI component improperly discloses the contents of its memory (CVE-2016-0168, CVE-2016-0169).
- A remote code execution vulnerability exists when the Windows GDI component fails to properly handle objects in memory (CVE-2016-0170).
- A use after free vulnerability in could allow for remote code execution when the Windows GDI component fails to properly handle objects in memory (CVE-2016-0184).
- A memory corruption vulnerability exists in Windows when the Windows Imaging Component fails to handle objects in memory (CVE -2016-0195).

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

Microsoft:
https://technet.microsoft.com/en-us/library/security/ms16-055

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0168
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0169
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0170
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0184
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0195